Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method of tracking incoming transmissions comprising:

identifying an incoming transmission including at least one identifiable portion;

computing, for each identifiable portion in the incoming transmission, a fingerprint indicative of the at least one identified portion, the fingerprint being substantially unique to the at least one identified portion;

storing the computed fingerprint to generate a set of stored fingerprints;

receiving a set of comparison fingerprints corresponding to a known portion of the incoming transmission, the set of comparison fingerprints being predetermined;

comparing the set of stored fingerprints to the set of comparison fingerprints to identify stored fingerprints matching at least one of the set of comparison fingerprints and, if a match is found, identifying a previous incoming transmission corresponding to a matching stored fingerprint of the set of stored fingerprints;

storing an indication of a subsequent disposition of the incoming transmission;

receiving a subsequent set of comparison fingerprints, the subsequent set of comparison fingerprints indicative of refinements to the known portion of the incoming transmission;

matching the subsequent set of comparison fingerprints to the stored fingerprints;

determining, based on the matching of the subsequent set of comparison fingerprints, if the subsequent set of comparison fingerprints is indicative of an undesirable portion in the incoming transmission; and

selectively performing, based on the determining, a remedial action in response to the subsequent disposition.

2. (Previously Presented) The method of claim 1 wherein storing further comprises selectively storing, if the incoming transmission does not correspond to the set of

comparison fingerprints, at least one fingerprint corresponding to the at least one identifiable portion of the incoming transmission.

3. (Original) The method of claim 1 wherein computing the fingerprint value includes determining a signature and comparing comprises signature matching.

4. (Original) The method of claim 1 further comprising receiving at least one successive set of comparison fingerprints, and iteratively comparing the successive sets of comparison fingerprints to the stored fingerprints, wherein if a match is found, identifying a distribution set of the incoming message corresponding to the matching stored fingerprint and transmitting an indication of the match to the distribution set.

5. (Previously Presented) The method of claim 1 wherein the set of comparison fingerprints are virus signatures computed from known undesirable transactions.

6. (Canceled)

7. (Previously Presented) The method of claim 1 wherein the subsequent disposition includes transmitting the incoming transmission to a list of successive recipients; and the remedial action is sending a notification to the successive recipients indicative of the matching incoming transmission.

8. (Original) The method of claim 1 wherein the incoming transmission further comprises a series of potentially harmful network transmissions, each of the incoming transmission operable to include malicious code, wherein the subsequent disposition includes delivery to at least one successive recipient and remedial action includes determining the successive recipients from the stored successive disposition and notifying each of the successive recipients.

9. (Original) The method of claim 1 wherein the determined undesirable portion did not indicate undesirable transmissions based on the comparing of a previous set of comparison fingerprints.

10. (Original) The method of claim 1 further comprising demarcating the incoming transmission into segments, each segment operable to yield a fingerprint, wherein comparing further comprises comparing each value in the set of comparison fingerprints with at least one of the segments.

11. (Previously Presented) The method of claim 10 further comprising

identifying a segment type of each segment, the segment type corresponding to the content included in the segment; and

categorizing each of the segments according to a heuristic, the heuristic indicative of a likelihood of the categorized segment including an undesirable transmission.

12. (Original) The method of claim 11 further comprising:

identifying a risk assessment of each of the segment types; and

storing the segment according to the identified risk assessment, storing further including identifying a duration.

13. (Original) The method of claim 12 wherein storing the segments further comprises storing the content of the segment with the corresponding fingerprint.

14. (Original) The method of claim 1 wherein the undesirable portions are selected from the group consisting of viruses, worms and Trojan horses included as an attachment according to an established mail protocol.

15. - 29. (Canceled)

30. (Previously Presented) A computer program product having a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for tracking incoming transmissions comprising:

computer program code for identifying an incoming transmission including at least one identifiable portion;

computer program code for computing, for each identifiable portion in the incoming transmission, a fingerprint indicative of the at least one identified portion, the fingerprint being substantially unique to the at least one identified portion;

computer program code for storing the computer fingerprint to generate a set of stored fingerprints;

computer program code for receiving a set of comparison fingerprints corresponding to known portion of the incoming transmission, the set of comparison fingerprints being predetermined;

computer program code for comparing the set of stored fingerprints to the set of comparison fingerprints to identify stored fingerprints matching any of the set of comparison fingerprints and, if a match is found, identifying a previously received incoming transmission corresponding to a matching stored fingerprint of the set of stored fingerprints;

computer program code for storing an indication of a subsequent disposition of the incoming transmission;

computer program code for receiving a subsequent set of comparison fingerprints, the subsequent set of comparison fingerprints indicative of refinements to the known portion of the incoming transmission;

computer program code for matching the subsequent set of comparison fingerprints to the stored fingerprints;

computer program code for determining, based on the matching of the subsequent set of comparison fingerprints, if the subsequent set of comparison fingerprints is indicative of an undesirable portion in the incoming transmission; and

computer program code for selectively performing, based on the determining, a remedial action in response to the subsequent disposition.

31. - 32. (Canceled)

33. (Previously Presented) The method of claim 1, wherein the identifying a previous incoming transmission corresponding to a matching stored fingerprint of the set of stored fingerprints is a retroactive analysis of a previously accepted transmission.

34. (Canceled)